IN THE CLAIMS:

1. (Previously presented) A method of documenting delivery and content of an electronic message, comprising:

receiving an electronic message from a message sender, the electronic message having at least one designated electronic delivery address associated therewith;

transmitting the electronic message to said designated address;

receiving electronic delivery status notification information regarding delivery of the electronic message to the designated address;

computing a message authentication code corresponding to at least the message; assembling a copy of at least a portion of the message, the electronic delivery status notification information, and the message authentication code, said assemblage defining an electronic receipt; and

transmitting the receipt to a storage means.

2. (Previously presented) The method of claim I wherein transmitting the receipt to a storage means comprises transmitting the receipt to the message sender.

3. (Previously presented) The method of claim 2 further comprising the step of discarding the original message after transmitting the electronic receipt to the sender.

4. (Previously presented) The method of claim I further comprising at a later time:

receiving a purported receipt and a purported message authentication code associated therewith;

determining that the purported message authentication code corresponds to the message; and

providing sworn testimony verifying content and delivery of the message to the addressee.

5. (Previously presented) The method of claim I wherein said sworn testimony is provided for a fee.

6. (Previously presented) The method of claim I wherein the message authentication code corresponds additionally to delivery status and delivery time information.

7. (Previously presented) The method of claim I wherein the step of computing an authentication code comprises:

computing a first message digest corresponding to at least a body of the message; computing a second message digest corresponding to an attachment to the message;

computing an overall message digest corresponding to said first and said second message digests; and

encrypting said overall message digest to create a digital fingerprint.

8. (Previously presented) The method of claim I wherein computing a message authentication code comprises:

using a secure hashing algorithm, computing a message digest corresponding to at least the message and the electronic delivery status notification information.

9. (Previously presented) The method of claim I wherein said transmitting step comprises:

establishing a direct telnet connection with an e-mail server associated with the destination address; and

transmitting the message directly to said e-mail server.

10. (Previously presented) The method of claim I further comprising the step of tagging the message to indicate that it has been registered with a third party prior to said step of transmitting the message to said designated address.

11. (Previously presented) The method of claim 1, wherein:

said step of receiving an electronic message comprises receiving the electronic message as an e-mail cc; and

the electronic delivery address is determined by examining a delivery address designated within a header associated with the message.

12. (Previously presented) A method of providing proof regarding the delivery and content of an electronic message, comprising:

receiving from a sender across a computer network an electronic message, said message having a delivery address associated therewith;

sending said message electronically to a destination corresponding to said delivery address;

receiving delivery status notification information associated with said message and said delivery address;

providing to said sender:

a substantial copy of said message;

said delivery status notification information; and

a message digest computed substantially from said message copy and said delivery status notification information; and

at a future date receiving electronically said electronic receipt from said sender, verifying that said message digest corresponds to said message, and verifying that said message was received by an electronic message handler associated with said delivery address.

13. (Previously presented) An electronic message server programmed to implement the method of claim 12.

14. (Previously presented) A computer readable memory capable of causing a computer to implement the method of claim 12.

15. (Previously presented) The method of claim 12 further comprising:

sending said message to a plurality of additional destinations corresponding to additional delivery addresses associated with the message;

receiving additional delivery status notification information associated with said message and said additional delivery addresses; and

sending a delivery verification message to the sender, the delivery verification message including:

a list of all of said addresses; and

said delivery status notification information respectively corresponding to all of said addresses, said delivery status notification information including for each addressee a listing of whether or not delivery was successful and, if delivery was successful, the date and time at which delivery occurred.

16. (Previously presented) The method of claim 12 wherein said computer network is the Internet and said electronic message is an e-mail message.

17. (Previously presented) The method of claim 12 wherein the step of sending said message electronically to a destination corresponding to said delivery address comprises:

establishing direct communication to a recipient electronic message server corresponding to said destination; and

sending said electronic message directly to said recipient electronic message server; and

verifying that said recipient electronic message server reported receiving said electronic message without errors.

18. (Previously presented) The method of claim 17 wherein said direct communication comprises a telnet connection across the Internet.

19. (Previously presented) The method of claim 12, wherein said message digest is encrypted.

20. (Previously presented) The method of claim 12, further comprising:

for a fee, providing sworn testimony verifying content of said message and receipt thereof at said delivery address.

21. (Previously presented) The method of claim 12, wherein said message digest includes:

a first message digest computed according to a body of said message; and

a second message digest computed according to an attachment to said message.

22. (Previously presented) The method of claim 12, wherein said message digest comprises a first message digest computed according to a body of said message and at least one electronic attachment to said message.

23. (Currently amended) A method of verifying delivery of an electronic message from a message originator to a plurality of destinations, comprising:

receiving an e-mail message, said e-mail message including a plurality of destination e-mail addresses associated therewith and a message originator address associated therewith;

forwarding said message to said plurality of addresses; providing a report to said message originator, the report listing whether the message was successfully transmitted to a computer associated with each respective destination address, and if the message was successfully transmitted, the date and time at which the e-mail was successfully received by the computer associated with the respective destination address.

24. (Previously presented) The method of claim 23 wherein the message is received from the sender across the Internet; the report is sent to the sender across the Internet, and wherein the method further comprises:

charging a fee to said message originator.

25. (Previously presented) A method of verifying delivery of an electronic message, comprising:

in a computer system, receiving an electronic message from a message sender for routing to a destination address;

establishing communication With an electronic message server associated with the destination address, said server defining a destination server;

querying said destination server to determine whether said destination server supports delivery status notification (DSN) functionality;

receiving a response to said query, said query and response together defining an SMTP dialog;

requesting delivery status notification information from said destination server according to results of said SMTP dialog;

transmitting said electronic message to said destination address;

receiving DSN information from said destination server with respect to delivery of said electronic message; and

providing to said message sender at least a portion of said SMTP dialog, and at least a portion of said DSN information.

26. (Previously presented) The method of claim 25, wherein the providing step includes composing an electronic receipt, said electronic receipt including:

a copy of said electronic message;

at least a portion of said SMTP dialog and at least a portion of said DSN information; and

a message authentication code corresponding to content of said receipt.

27. (Previously presented) A method of verifying content of a received electronic message, comprising:

registering a designated server as the recipient for messages addressed to e-mail

addresses at a plurality of top level domains;

receiving an electronic message addressed to a first e-mail address within said plurality of top level domains;

generating a message authentication code corresponding to content of said received message and delivery information associated with said message;

providing the message and the message authentication code to a recipient associated with said first e-mail address;

at a later time, verifying that said message digest corresponds to said message and delivery information.

28. (Previously presented) The method of claim 27 wherein said message authentication code comprises an encrypted message digests.

29. (Previously presented) The method of claim 27 wherein said providing comprises POP mail service.

30. (Previously presented) The method of claim 27 wherein said message authentication code and said message are combined into a single delivered message provided to said designated addressee.

31. (Previously presented) A method of verifying delivery and reading of an electronic message, comprising:

receiving an electronic message across the Internet from a message sender, said message including an electronic destination address;

forwarding said message to a destination server associated with said destination address;

requesting delivery status notification from said destination server;

receiving confirmation from said destination server that said message was received;

sending to the message sender at least one receipt, said at least one receipt including:

delivery information, said delivery information including the time at which the message was received;

read notification information regarding when a user at said destination address opened said electronic message for reading; and at least one message authentication code corresponding to the message, the delivery information, and the read notification information.

32. (Previously presented) The method of claim 31 wherein said at least one receipt comprises:

a first receipt, said first receipt comprising said delivery information and a first message authentication code associated therewith; and

a second receipt, said second receipt comprising said read notification information and a second message authentication code associated therewith.

33. (Previously presented) A method of verifying that an electronic message was sent, comprising:

generating an electronic message for a recipient from information received from a message originator;

sending the electronic message to the recipient;

generating a message digest corresponding to content of the electronic message; encrypting the message digest; and

sending the electronic message and the encrypted digest to the message originator.

34. (Previously presented) The method according to claim 33, further comprising:

tracking delivery status notification of the message;

appending the delivery status notification to the electronic message; and

storing the appended delivery status notification for later verification if needed.

35. (Previously presented) The method according to claim 33, wherein the electronic message is sent to the recipient through a computer network.

36. (Previously presented) The method according to claim 35, wherein the computer network is a wide area network.

37. (Previously presented) The method according to claim 35, wherein the computer network is the Internet.

38. (Previously presented) A method of later proving that an electronic message was previously sent to a recipient, comprising:

receiving from an independent party an electronic message, and further receiving an address corresponding to an intended recipient of the message;

creating a validation code corresponding to the message;

transmitting the validation code to a storage means for storage thereat; and sending the message to the recipient.

39. (Previously presented) The method of claim 38 wherein said storage means comprises said independent party.

40. (Previously presented) The method according to claim 38 wherein said storage means comprises an on-site memory device.

41. (Previously presented) The method according to claim 38 wherein said validation code is a message digest.

42. (Previously presented) The method according to claim 41 further comprising:

encrypting the message digest;

creating a receipt, the receipt including the encrypted message digest; and forwarding the receipt to the independent party for later verification if needed.

43. (Previously presented) A method of establishing whether a message was electronically received by a recipient, comprising:

providing a message to be dispatched electronically along with a recipient's address from a sender;

dispatching the message electronically to the recipient's address;

upon receiving a delivery status of the message, generating a receipt, the receipt including:

a copy of the message;

a digital signature associated with the message; and the delivery status for the message; and

providing the receipt to the sender, for later establishing that the message was electronically received by the recipient.

44. (Previously presented) The method of claim 43 wherein the digital signature is an encrypted message digest.

45. (Previously presented) The method of claim 43, wherein the message is an e-mail message.

46. (Previously presented) The method of claim 43, wherein the digital signature is a message digest corresponding to the message.

47. (Previously presented) The method of claim 43, wherein the message is dispatched via the Internet.

48. (Previously presented) The method of claim 43, wherein the message is provided by logging onto a registrant's server to create an e-mail message for the recipient.

49. (Previously presented) The method of claim 43, wherein the status of the message is a Delivery Status Notification.

50. (Previously presented) The method of claim 43, wherein tracking for the delivery status of the message dispatched is done for a period of up to about 24 hours.

51. (Previously presented) The method of claim 43, wherein tracking for the delivery status of the message occurs for more than about 24 hours, and the receipt records that delivery of the message is a delivery failure.

52. (Previously presented) The method of claim 43, wherein the receipt further includes the time that the message was received at the recipient's address.

53. (Previously presented) The method of claim 43, wherein the message includes an attached file, and

wherein the method rather comprises:

creating a message digest associated with the attached file; and encrypting the message digest; and

wherein said dispatching step includes dispatching the message including the attached file.

54. (Previously presented) The method of claim 43, further including:

sending the receipt to the sender of the message.

55. (Previously presented) The method of claim 43, further comprising:

requesting a reading receipt from the recipient; and

if the request for a reading receipt is responded to by the recipient, generating a second digital signature corresponding to the contents of the reading receipt and sending the second digital signature to the sender.

56. (Previously presented) A method of proving that an electronic message sent to a recipient was read, comprising:

receiving an electronic message along with a recipient's address;

calculating a message digest corresponding to the electronic message;

dispatching the electronic message electronically to the recipient's address;

requesting a reading notification;

upon receiving the reading notification, generating at least one reading receipt, the at least one reading receipt including:

a copy of the message;

a first message digest for the corresponding electronic message; and

a second message digest for the reading notification from the recipient; and

providing the reading receipt for later verification that said message was received by the recipient.

57. (Previously presented) The method of claim 56 wherein the electronic message is provided by logging onto a registrant's server to create an e-mail message for the recipient by a sender.

58. (Previously presented) The method of claim 57, further including:

sending the reading receipt to the sender of the electronic message.

59. (Previously presented) The method of claim 56, further including:

appending to the reading receipt any files accompanying the reading receipt; and generating respective message digests for any of the accompanying files.

60. (Previously presented) A method of validating the integrity of a purported copy of an electronic message, comprising:

receiving said purported electronic message copy, said purported copy including a digital signature and a transmission history associated therewith;

decrypting the digital signature;

generating a message digest based on content of the purported copy; and

validating the purported copy by comparing the decrypted digital signature and the message digest to determine whether the two match.

61. (Previously presented) The method according to claim 60, further comprising:

if requested, providing sworn testimony verifying the content of the electronic message.

62. (Previously presented) A method of registering an inbound electronic message, comprising:

generating a message digest corresponding to an inbound electronic message being sent to a recipient's address;

encrypting the message digest to create a digital signature;

appending the message digest to the contents of the inbound electronic message to create a receipt;

transmitting the electronic message to the recipient address; and sending the receipt to an archival storage means.

63. (Previously presented) The method according to claim 62 wherein the electronic message is an e-mail.

64. (Previously presented) A method of registering an e-mail, comprising:

generating a message digest for content corresponding to the e-mail; encrypting the message digest;

appending the encrypted message digest to the content of the e-mail to create a receipt-sending the e-mail; and

transmitting the receipt to a storage means for storage thereat.

65. (Previously presented) A method of documenting delivery of an e-mail message comprising:

receiving an e-mail message from a sender;

forwarding the message to at least one designated recipient;

recording delivery information associated with the forwarding of the message to each designated recipient;

computing a message digest corresponding to the said message and delivery information;

transmitting the message digest to the sender;

discarding the message; and

at a later time, examining said message, said delivery information, and said message digest, and providing third party verification services attesting that said message was sent to the designated recipient at the time indicated within the delivery information.

66. (Previously presented) The method of claim 65, further comprising:

performing the steps recited in claim VK I for each of a plurality of unrelated entities, thereby providing independent third party e-mail authentication and verification services for said entities.

67. (Previously presented) The method of claim 65 further comprising:

programming a message transport agent associated with said sender to redirect outgoing e-mail message originally addressed to said designated recipient, to a designated third party, and to alter said message to include said designated recipient's e-mail address; and

wherein said third party performs said forwarding, recording, computing, and transmitting steps.

68. (Previously presented) The method of claim 67 further comprising:

providing a flag which a message sender can set in order to designate a particular outgoing message as a message to be registered.

69. (Previously presented) The method of claim 65 further comprising:

advising the designated recipient that the message has been registered with a third party verification service.

70. (Previously presented) The method of claim 65, further comprising:

charging the message sender a fee, said fee selected from the group comprising of a monthly fee, another periodic fee, a fee based on amount of data registered, and a per-message fee.

71. (Previously presented) The method of claim 65, wherein said attesting is performed for a fee.

72. (Previously presented) An electronic receipt for delivery of an electronic message, said receipt comprising:

a body of an electronic message;

delivery information pertaining to a date and time that the electronic message body was delivered to a computer associated with a designated addressee; and

a message authentication code computed from said message body and said delivery information, said message authentication code being computed by an independent entity.

73. (Previously presented) A method of providing electronic message registration services to the public, comprising:

providing a worldwide web site at which a user can input a message and designate a recipient by entering the recipient's electronic address;

receiving the message and the recipient's address via said website;

forwarding the message to the recipient's electronic address; and providing secure documentation to the user pertaining to:

the message content; and

the date and time at which the message was forwarded to the recipient's electronic address.

74. (Previously presented) The method of claim 73 further comprising:

receiving delivery confirmation from a computer associated with said recipient's electronic address, and including said delivery confirmation as part of said secure documentation.

75. (Previously presented) The method of claim 74 further comprising:

receiving reading receipt information regarding when the designated recipient opened the electronic message for reading, and including said reading receipt information as part of said secure documentation.

76. (Previously presented) A method of providing e-mail message documentation services,

comprising: receiving an e-mail message from a message sender;

creating a copy of the message and appending to the message copy a tag advising that the message has been registered with a third party e-mail registration service;

forwarding the tagged copy to a designated addressee; and

providing secure documentation to the message sender regarding content of the message and delivery status information associated therewith.

77. (Previously presented) A method of documenting delivery and content of an electronic message comprising:

recording electronic message protocol exchanges that effect delivery of the message to a destination mail transport authority (MTA);

assembling a copy of at least a first portion of the message, the protocol exchange, an authentication code corresponding to at least a second portion of the message, said assemblage defining an electronic receipt; and

transmitting the receipt to a storage means.

78. (Previously presented) The method of claim 77 wherein said protocol exchanges comprise simple mail transport protocol (SMTP) exchanges.

79. (Previously presented) The method of claim 77 further comprising:

assigning a fictitious return address to the message in such a way that a receiving MTA will return delivery status notification (DSN) with sufficient information so as to enable determination of which message and which destination the DSN concerns merely by analysis of the DSN's return address and without otherwise relying on content of said message.

80. (Previously presented) The method of claim 77 further comprising:

scanning subject lines and bodies of a return MTA notification to determine, by the presence of indicative phrases, whether the MTA notification reports a successful delivery, a failed delivery, or the relay of the message to anon extended simple mail transport protocol (ESMTP) complaint mailer.

81. (Previously presented) The method of claim 77 further comprising:

assembling and delivering a delivery report which, for each successful delivery of the message indicates whether the system is only able to verify on the basis of said recorded protocol exchanges, delivery of said message to a destination's mail server or, alternatively, whether the system is able to verify on the basis of an MTA notification, delivery of the message to an electronic mailbox corresponding to the destination.

82. (Previously presented) A method of tracking delivering of a particular electronic message comprising:

assigning a fictitious return address to the message, the fictitious return address containing sufficient information to identify the original message; and requesting message delivery status notification so as to cause a device which receives the message to report delivery status information to the fictitious return address.

83. (Previously presented) The method of claim 82 wherein:

said fictitious return address contains sufficient information to identify content of the message.

84. (Previously amended) A method of transmitting a message through the internet from a sender to a recipient through a server displaced from the recipient, including the steps at the server of:

receiving the message at the server from the sender, transmitting, through the internet from the server to an agent of the recipient, the message, an identification and an internet address of the server and the identity of the sender of the message,

receiving from the agent at the server through the internet the identity and address of the agent and an indication of the receipt by the agent of the message and the identification and internet address of the server and the identity of the sender, and

sending to the sender from the server through the internet a copy of the message and the information received by the server from the agent and a digital signature of the message received by the server from the agent of the recipient.

85. (Previously presented) A method of transmitting a message through the internet from a sender to a recipient through a server displaced from the recipient, including the steps at the server of:

receiving the message at the server from the sender,

transmitting, through the internet from the server to an agent of the recipient, the message, an identification and an internet address of the server and the identity of the sender of the message,

receiving from the agent at the server through the internet the identity of the agent and an indication of the receipt by the agent of the message and the identification and internet address of the server and the identify of the sender and the digital fingerprint of the message, and sending to the sender from the server through the internet a copy of the message and the information received by the server from the agent.

86. (Previously amended) A method as set forth in claim 84 wherein

the server identifies any attachment to the message and wherein

the identity of the attachment is received by the server through the internet from the agent and wherein

the server sends to the sender through the internet a copy of the attachment received from the agent and a digital signature of the attachment.

87. (Previously amended) A method as set forth in claim 84 wherein

a digital signature of the message is provided at the server by a plurality of digits in a unique sequence and is sent by the server to the sender.

88. (Previously presented) A method as set forth in claim 84 wherein

a digital fingerprint of the message is provided at the server by a plurality of digits in a unique sequence and is sent by the server to the sender.

89. (Previously presented) A method as set forth in claim 84 wherein

the server creates a message digest of the message and encrypts the message digest and sends the encrypted message digest to the sender through the internet with the message, the identification and e-mail address of the server and the identity of the sender.

90. (Previously amended) A method of transmitting a message through the internet from a sender to a recipient through a server displaced from the recipient, including the steps at the server of:

receiving the message at the server from the sender,

transmitting from the server through the internet to an agent of the recipient the message and the identity and internet address of the server and an indication representing the identity of the sender,

receiving at the server from the agent a handshaking and delivery history of the message from the server to the agent, and

transmitting from the server to the sender through the internet the message, a digital signature, including a digital signature, of the message and the handshaking and delivery history of the message received by the server from the agent.

91. (Previously amended) A method as set forth in claim 90 wherein

the server receives from the sender a copy of the information previously sent by the server to the sender, this information including the digital signature and the message, when the sender wishes to have the message authenticated by the server and wherein the server does not retain a copy of the any of the information transmitted from the server to the sender, after the server transmits to the sender through the internet the message, the digital signature of the message and the handshaking and delivery history of the message.

92. (Previously amended) A method as set forth in claim 91 wherein

the server receives from the sender the information previously transmitted by the server to the sender and wherein

the server uses the information received by the server from the sender to create a digital signature and compares this digital signature with the digital signature received by the server from the sender to authenticate the message received by the server from the sender.

93. (Previously presented) A method as set forth in claim 90 wherein

the server retains a copy, except for the message, of the information received by the server from the agent and sent to the sender and wherein

when the sender wishes to authenticate that the message was sent by the server to the agent, the server matches the information, except for the message, sent by the server to the sender relating to the message with the information retained by the server relating to the message.

94. (Previously presented) A method as set forth in claim 90 wherein

the message includes an attachment and wherein

the server receives the attachment from the sender and wherein

the server transmits the attachment to the agent at the same time that the sender transmits the message to the agent and wherein

the server receives from the agent the attachment at the same time that it receives the message and the handshaking and delivery history of the message from the agent and wherein

the server transmits the attachment and a digital signature, including a digital fingerprint, of the attachment to the sender at the same time that it transmits the digital signature of the message to the sender.

95. (Previously presented) A method as set forth in claim 90 wherein

the message is transmitted from the sender to the agent in an individual one of a variety of recognized header formats and wherein

the server receives from the agent the digital signature of the message and the handshaking and delivery history of the message with the header formed in the individual one of the variety of recognized header formats.

96. (Previously presented) A method as set forth in claim 90 wherein

the server requests a delivery status notification from the agent relating to the message when it transmits the message to the agent and wherein the server receives the delivery status notification from the agent when it receives the digital signature of the message from the agent.

97. (Previously amended) A method as set forth in claim 93, including the steps at the server of:

receiving from the sender at the server through the internet, at the same time as the receipt of a copy of the message from the sender to the server, a copy of any attachment to the message, and

providing for a transmittal from the agent to the server through the internet of the attachment at the same time as the transmittal of the message from the agent to the server.

98. (Previously amended) In a method of transmitting a message through the internet from a sender to a recipient through a server displaced from the recipient, the steps at the server of:

receiving the message at the server from the recipient,

generating a hash constituting a synopsis of the message in coded form,

encrypting the hash with a particular encryption code to generate a digital signature of the message, and

transmitting the message and the digital signature of the message through the internet to the sender.

99. (Previously amended) In a method as set forth in claim 98, the steps at the server of:

generating, for any attachment to the message, a hash constituting a synopsis of the attachment in coded form,

encrypting the hash with a particular encryption code to generate a digital signature of the attachment, and

transmitting the attachment and the digital signature of the attachment to the sender through the internet at the same time that the message and the digital signature of the message are transmitted from the server to the sender through the internet.

100. (Previously amended) In a method as set forth in claim 98, the steps at the server of:

removing the message and the digital signature of the message from the server after the transmission of the message and the digital signature of the message from the server to the sender.

101. (Previously amended) In a method as set forth in claim 99, the steps at the server of:

removing the message and the digital signature of the message from the server after the transmission of the message and the digital signature of the message from the server to the sender, and removing the attachment, and the digital signature of the attachment, from the server after the transmission of the attachment, and the digital signature of the attachment, from the server to the sender.

102. (Previously amended) In a method as set forth in claim 98, the step at the server of:

receiving at the server from the sender the message, and the digital signature of the message, previously transmitted from the server to the sender.

103. (Previously amended) In a method as set forth in claim 101, the step of:

authenticating the message on the basis of the message, and the digital signature of the message, transmitted from the sender to the server.

104. (Previously amended) In a method as set forth in claim 102, the step of:

authenticating at the server the message received by the server from the sender on the basis of the message, and the digital signature of the message, transmitted from the sender to the server, the authentication being provided by generating the digital signature of the message received by the server from the sender and by comparing the generated digital signature and the received digital signature.

105. (Previously amended) In a method as set forth in claim 103, the step of:

authenticating at the server the message received by the server from the sender on the basis of the message, and the digital signature of the message, transmitted from the sender to the server, the authentication being provided by generating the digital signature of the message received by the server from the sender and by comparing the generated digital signature and the received digital signature and by indicating the authentication when the generated digital signature and the received digital signature are the same.

106. (Previously amended) In a method of transmitting a message through the internet from a sender to an agent for the recipient through a server displaced from the agent, the steps at the server of:

receiving the message at the server from the sender,

transmitting the message and the identity of the sender and the identity and internet address of the server through the internet from the server to the agent,

receiving at the server through the internet any transmission through the internet from the agent concerning the message from the sender, and

determining from the transmission received by the server from the agent, or from the lack of any reception by the server through the internet from the agent, the delivery status of the transmission by the server to the agent and the delivery status of any delivery of the message by the agent to the recipient.

107. (Previously amended) In a method as set forth in claim 106, the steps at the server of:

periodically examining the delivery status of the message transmitted to the agent and the status of any delivery of the message by the agent to the recipient, and

transmitting the message and the digital signature of the message and the identity of the sender and the identity and internet address of the server through the internet to the sender with an indication of the delivery of the message to the agent when the server determines from the periodic examination that the message has been delivered to the transport agent.

108. (Previously amended) A method of transmitting a message through the internet from a sender to an agent for a recipient through a server displaced from the agent, including the steps at the server of:

receiving the message at the server,

transmitting through the internet to an agent of the recipient the message and the identity of the sender and the identity and the internet address of the server,

receiving from the agent the message and the identity and internet address of the agent and the identity of the sender and the identity and internet address of the server,

providing a digital signature of what was received from the agent, and

providing to the sender the information received by the server from the agent and the digital signature of the information received by the server.

109. (Previously amended) A method as set forth in claim 108, including the steps at the server of:

providing to the sender the message at the same time as the provision of the digital signature of the message to the sender, and

discarding the message provided to the sender.

110. (Previously amended) A method as set forth in claim 108, including the steps at the server of:

receiving from the agent [providing] an indication of the date and time of the reception by the agent of the identity and internet address of the agent and the identity of the sender and the identity and the internet address of the server, and

providing to the sender the indication of the date and time of the reception by the agent of the identity and internet address of the agent and the identity of the sender and the identity and internet address of the server.

111. (Previously amended) A method as set forth in claim 108, including the steps at the server of:

receiving from the sender a copy of the message provided by the server and a copy of the digital signature of the message and the identity and internet address of the agent and the identity of the sender and the identity and internet address of the server,

generating a digital signature of what has been received from the sender, comparing the digital signature received by the sender and the digital signature generated by the server, and

authenticating the message received from the sender on the basis of the comparison provided at the server.

112. (Previously amended) A method as set forth in claim 108, including the steps at the server of:

forming at the server the digital signature of the message by providing a hash of the message and then

encrypting the hash of the message.

113. (Previously amended) A method as set forth in claim 108, including the steps at the server of:

providing a digital signature of an attachment to the message,

transmitting to the agent the attachment at the same time as the transmittal of the message, and

transmitting to the sender the digital signature of the attachment at the same time as the transmission of the digital signature of the message to the sender.

114. (Previously amended) A method as set forth in claim 112, including the steps at the server of:

providing an indication of the date and time of the reception of the message from the agent, and

providing to the sender the indication of the date and time of providing to the server the digital signature of the message from the agent at the time of providing to the sender the digital signature of the message,

providing to the sender the message at the same time as the provision of the digital signature of the message to the sender, and

discarding the message provided to the sender,

providing a digital signature of an attachment to the message,

transmitting to the sender the attachment at the same time as the transmittal of the message to the sender,

transmitting to the sender the digital signature of the attachment at the same time as the transmission of the digital signature of the message to the sender,

receiving from the sender a copy of the message provided to the sender and a copy of the digital signature of the message and the identity and internet address of the agent and the identity of the sender and the identity and internet address of the server,

generating a digital signature of what has been received from the sender relating to the message,

comparing the digital signature received from the sender and the digital signature generated on the basis of what has been received from the sender relating to the message, and authenticating the message received from the sender on the basis of the comparison provided by the server.

115. (Currently amended) In a method of transmitting [[~~a~~]] an unencrypted message [[,]] from a sender to a destination address through a server displaced from the destination address the steps at the server of:

receiving the unencrypted message from the sender,

transmitting the unencrypted message, without any encryption, to the destination address,

receiving at the server an indication from the destination address that the message has been received at the destination address from the server,

without encrypting the unencrypted address, providing at the server a digital signature of the unencrypted message, and

transmitting to the sender the unencrypted message [[,]] and the digital signature of the unencrypted message for storage by the sender.

116. (Currently amended) In a method as set forth in claim 115, the step at the server of:

discarding the unencrypted message and the digital signature of the unencrypted message after the transmission of the unencrypted message and the digital signature of the unencrypted message to the sender and before any authentication of the unencrypted message.

117. (Currently amended) In a method as set forth in claim 116, the steps at the server of:

receiving from the sender a copy of the unencrypted message and the digital signature of the unencrypted message before any authentication of the unencrypted message,

generating digital fingerprints of the unencrypted message and the digital signature received from the sender,

comparing the digital fingerprints, and

authenticating the unencrypted message on the basis of the results of the comparison.

118. (Currently amended) In a method as set forth in claim 116, the steps at the server of:

without encrypting the unencrypted message, providing at the server[[~~,]] at the same time as the provision of the digital signature of the message at the server,~~ an attachment including the identity of the sender and the identity and ~~internet~~ address of the server and the identity and ~~internet~~ the destination address of ~~the agent~~ a recipient, all as received by the server from the agent destination address,

generating a digital signature of the attachment without encrypting the unencrypted message, and

without encrypting the unencrypted message, transmitting to the sender the attachment including the identity of the sender, the identity and ~~internet~~ address of the server and the identity and ~~internet~~ destination address of the [[~~agent~~]] recipient and the digital signature of the attachment, all as received by the server from the ~~agent~~ destination address, at the same time as the transmission of the message, and the digital signature of the message, to the sender.

119. (Currently amended) In a method as set forth in claim 115, the steps at the server of:

receiving an attachment from the destination address without encrypting the unencrypted message,

without encrypting the unencrypted message, providing at the server a digital signature of the attachment,

without encrypting the unencrypted message, transmitting to the sender~~, at the same time as the transmission of the message and the digital signature of the message,~~ the attachment and the digital signature of the attachment without encrypting the unencrypted message.

120. (Currently amended) In a method as set forth in claim 115, the steps at the server of:

without encrypting the unencrypted message, receiving from the sender copies of the unencrypted message and the attachment and the digital signatures of the unencrypted message and the attachment, without encrypting the unencrypted message, generating digital fingerprints of the unencrypted message and the digital signature of the unencrypted message and digital fingerprints of the attachment and [[of]] the digital signature of the attachment, and

comparing the digital fingerprints of the unencrypted message and the digital signature of the unencrypted message, and comparing the digital fingerprints of the attachment and the digital signature of the attachment, to authenticate the unencrypted message and the attachment.

121. (Currently amended) In a method as set forth in claim 119, the steps at the server of:

without encrypting the unencrypted message, receiving the unencrypted message and the digital signature of the unencrypted message at the server from the sender, and

authenticating the unencrypted message at the server on the basis of the unencrypted message and the digital signature received by the server from the sender.

122. (Previously amended) A method of transmitting a message through the internet from a sender to an agent for a recipient through a server displaced from the agent, including the steps of

providing the message from the sender at the server,

providing at the server a digital fingerprint of the message and the identity of the sender and the identity and internet address of the server, transmitting to the agent the message and the identity of the sender and the identity and the internet address of the server,

providing at the agent an indication of the status of the reception at the agent of the transmittal from the server to the agent of the message and the identity of the sender and the identity and interest address of the server, and

transmitting to the server from the agent the identity and internet address of the agent and the status of the reception at the agent of the message and the identity of the sender and the identity and internet address of the server.

123. A method as set forth in claim 122, including the steps of:

providing at the server a digital fingerprint of an attachment to the message,

transmitting the attachment to the agent at the same time as the transmittal of the message to the agent,

providing at the agent the status of the reception of the attachment at the same time as the provision at the agent of the status of the reception of the message, and

transmitting to the server from the agent the status of the reception of the attachment at the same time as the transmittal to the server from the agent of the status of the reception of the message.

124. A method as set forth in claim 122 wherein

the digital fingerprint of the message includes a digital digest of the message and an encryption of the digital digest.

125. A method as set forth in claim 122 wherein

the agent includes in the transmission to the server the date and time of the transmission by the agent to the server.

126. A method as set forth in claim 122 wherein

the server transmits to the sender the message and the digital fingerprint of the message and the identity of the sender and the identity and internet address of the server and the identity and internet address of the agent and the status at the agent of the reception at the agent of the message.

127. A method as set forth in claim 122 wherein

the delivery status of the message at the agent includes at least one of the following: (a) DELIVERED, (b) RELAYED, (c) DELIVERED-AND-WAITING FOR DELIVERY STATUS NOTIFICATION (DSN), (d) DELIVERED-TO-MAILBOX, and (e) FAILED, UNDELIVERABLE.

128. (Previously amended) A method as set forth in claim 122 wherein

the digital fingerprint of the message includes a digital digest of the message and an encryption of the digital digest,

the agent includes the date and time of the transmission by the agent to the server, and the server transmits to the sender the message and the digital fingerprint of the message and the identity of the sender and the identity and internet address of the server and the identity and internet address of the agent and the status at the agent of the reception at the agent of the message and the digital fingerprint of the message,

the delivery status of the message at the agent includes at least one of the following: (a) DELIVERED, (b) RELAYED, (c) DELIVERED-AND-WAITING FOR DELIVERY STATUS NOTIFICATION (DSN), (d) DELIVERED-TO-MAILBOX, and (e) FAILED, UNDELIVERABLE.

129. A method as set forth in claim 128, including the steps of:

providing at the server a digital fingerprint of an attachment to the message,

transmitting the attachment to the message to the agent at the same time as the transmittal of the message to the agent,

providing at the agent the status of the reception of the attachment at the same time as the provision at the agent of the status of the reception of the message, and

transmitting to the server from the agent the status of the reception of the attachment at the same time as the transmittal to the server from the agent of the status of the reception of the message.

130. (Previously amended) A method of transmitting a message through the internet from a sender to an agent for a recipient through a server displaced from the agent, including the steps at the server of:

providing at the server a digital fingerprint of the message and the identity of the sender and the identity and internet address of the server,

transmitting to the agent the message and the identity of the sender and the identity and internet address of the server,

receiving from the agent the identity of the sender and the identity and internet address of the server and the identity and internet address of the agent and an indication of the status of the reception of the message at the agent, and

transmitting to the sender the message and the information received by the server from the agent relating to the message.

131. A method as set forth in claim 130, including the steps at the server of:

providing at the server a digital fingerprint of an attachment to the message,

transmitting to the agent the attachment at the same time that the message is transported to the agent,

receiving from the agent the status of the reception at the agent of the attachment at the same time that the server receives from the agent the status of the reception at the agent of the message, and

transmitting to the sender the attachment and the information received by the server from the agent relating to the attachment at the same time that the server transmits to the sender the message and the information received by the server from the agent relating to the message.

132. A method as set forth in claim 130 wherein

the delivery status of the message at the agent includes at least one of the following: (a) DELIVERED, (b) RELAYED, (c) DELIVERED-AND-WAITING FOR DELIVERY STATUS NOTIFICATION (DSN), (d) DELIVERED-TO-MAILBOX, and (e) FAILED, UNDELIVERABLE.

133. A method as set forth in claim 130 wherein

the server receives from the agent the date and time of the transmission by the agent to the server of the status of the reception of the message at the agent and wherein

the server transmits to the sender the date and time of the transmission by the agent of the status of the reception by the agent of the message at the same time that the server transmits to the sender the status of the reception by the agent of the message.

134. A method as set forth in claim 133 wherein

the server also transmits to the sender the date and time of the transmission to the sender of the status of the reception by the agent of the message.

135. A method as set forth in claim 134 wherein

the server does not store the message after it transmits the message to the sender.

136. (Previously amended) A method as set forth in claim 134 wherein

the server transmits to the sender the identity of the sender and the identity and internet address of the server at the same time that it transmits the message and the digital fingerprint of the message to the sender and wherein

the server stores the identity of the sender and the identity and the internet address of the server and the digital fingerprint of the message and wherein

the server compares the stored identity of the sender and the identity and the internet address of the server, all as stored by the server, and the identity of the sender and the identity and the internet address of the server, all as received by the sender, to authenticate the message transmitted from the server to the sender.

137. (Previously amended) A method as set forth in claim 134 wherein

the server transmits to the sender the identity and internet address of the agent and the status of the reception of the message, all as received by the server from the agent, and the digital fingerprint of the message and wherein

the server stores the identity and internet address of the agent and the status of the reception of the message received by the agent, all as received by the server from the agent and the digital fingerprint of the message, and wherein

the server compares the stored identity and internet address of the agent and the status of the reception of the message and the digital fingerprint of the message with the identity and internet address of the agent and the status of the reception of the message and the digital fingerprint of the message all as received by the sender from the server, to authenticate the message transmitted from the server to the sender.

138. (Previously amended) A method as set forth in claim 136 wherein

the server does not store the message after it transmits the message to the sender and wherein

the server transmits to the sender the identity and internet address of the agent and the status of the reception of the message received by the agent, all as received by the server from the agent, and the digital fingerprint of the message, and wherein

the server stores the identity and internet address of the agent and the status of the reception of the message and the digital fingerprint of the message received by the agent, all as received by the server from the agent, and the digital fingerprint of the message and wherein

the server compares the stored identity and internet address of the agent and the status of the reception of the message and the digital fingerprint of the message with the identity and internet address of the agent and the status of the reception of the message and the digital fingerprint of the message, all as received by the sender from the server, to authenticate the message transmitted from the sender to the server.

139. (Previously presented) A method of authenticating a message transmitted through the internet from a sender to a recipient through a server displaced from the recipient, including the steps at the server of:

transmitting to the sender the message and a digital fingerprint of the message, and a status of the reception of the message by an agent for the recipient,

storing the digital fingerprint of the message at the server and the status of the reception of the message by the agent,

receiving from the sender the digital fingerprint of the message and the status of the reception of the message by the agent, and

comparing the stored digital fingerprint of the message and the digital fingerprint of the message as received by the server from the sender to authenticate the message transmitted from the server to the sender.

140. A method as set forth in claim 139 wherein

the server stores the information transmitted by the server relating to the status of the reception of the message and the digital fingerprint of the message but does not store the message and wherein

the server compares the information stored by the server, and the information provided by the sender, relating to the status of the reception by the agent of the message, and the digital fingerprint of the message, to authenticate the message transmitted by the server to the sender.

141. (Previously amended) A method as set forth in claim 139 wherein

the server transmits to the sender the identity of the sender and the identity and internet address of the server, all as transmitted by the agent to the server and wherein

the server stores the identity of the sender and the identity and internet address of the server, all as transmitted by the agent to the server and wherein

the server compares the information stored by the server, and the information provided by the sender, relating to the identity of the sender and the identity and information address of the server to authenticate the message transmitted by the server to the sender.

142. (Previously amended) A method of authenticating a message transmitted through the internet from a sender to an agent for a recipient through a server displaced from the agent, including the steps of:

transmitting to the sender the message and a digital fingerprint of the message and a status of a reception by an agent for the recipient of the message,

storing the digital fingerprint of the message at the server, and

comparing the stored digital fingerprint of the message and the digital fingerprint of the message transmitted to the sender to authenticate the message transmitted from the server to the sender.

143. The method as set forth in claim 142 wherein

the server does not store the message after it transmits the message to the sender.

144. A method as set forth in claim 142 wherein

the server transmits to the sender the identity of the sender and the identity and internet address of the server at the same time that it transmits the message and the digital fingerprint of the message to the sender and wherein

the server stores the identity of the sender and the identity and the internet address of the server at the same time that it transmits the message and the digital fingerprint of the message to the sender and wherein

the server receives from the sender the identity of the sender and the identity and internet address of the server and wherein

the server compares the identity of the sender and the identity and the internet address of the server, all as received by the server from the sender, with the stored identity of the sender and the stored internet address of the server to authenticate the message transmitted from the server to the sender.

145. (Currently amended) A method of transmitting a<u>n unencrypted</u> message from a sender to a destination address for a recipient through a server displaced from the destination address, including the steps at the server of,

receiving the unencrypted message from the sender without encrypting the unencrypted message,

transmitting the unencrypted message to the destination address through a path including servers between the server and the destination address, and

transmitting to the sender the unencrypted message and the path of transmission of the unencrypted message between the server and the destination address.

146. (Currently amended) A method as set forth in claim [[~~237~~]] 145 wherein

the server receives from the sender the unencrypted message and the path of transmission of the unencrypted message between the server and the destination address and wherein

the server authenticates the unencrypted message on the basis of the unencrypted message and the path of transmission of the unencrypted message between the server and the destination address without encrypting the unencrypted message.

147. (Currently amended) A method as set forth in claim 14[[~~6~~]][[5]] wherein

the server does not retain the unencrypted message after it transmits the unencrypted message to the sender before any authentication of the unencrypted message.

148. (Currently amended) A method as set forth in claim 145 wherein

the destination address is one of a plurality of destination addresses receiving the unencrypted message from the server and wherein the server distinguishes each of the destination addresses in the plurality in the transmission of the unencrypted message to the destination addresses in the plurality without encrypting the unencrypted message.

149. (Currently amended) A method as set forth in claim 145 wherein

the path of transmission of the unencrypted message between the server and the destination address includes the identity and address of the server and the identity of a recipient at the destination address.

150. (Currently amended) A method as set forth in claim 146 wherein

the server does not retain the unencrypted message after it transmits the unencrypted message to the sender before any authentication of the unencrypted message and wherein

the destination address is one of a plurality of destination addresses receiving the unencrypted message from the server and wherein

the server distinguishes each of the destination addresses in the plurality in the transmission of the unencrypted messages to the destination addresses in the plurality without encrypting the unencrypted message, and wherein

the message has an attachment and wherein

the attachment identifies the path of transmission of the unencrypted message between the server and the destination address without encrypting the unencrypted message.

159. (Currently amended) A method of providing a delivery at a server of an unencrypted electronic message from the server to a destination address, including the steps at the server of:

receiving at the server ~~the unencrypted~~ [[~~an~~]] the unencrypted electronic message from a sender for transmission to the destination address without encrypting the unencrypted electronic message,

transmitting the unencrypted electronic message from the server to the destination address via a protocol selected from a group consisting of an SMTP protocol and an ESMTP protocol without encrypting the unencrypted electronic message, and

receiving at the server the transmission of the electronic message between the server and the destination address via the selected one of the SMTP and ESMTP protocols without encrypting the unencrypted electronic message.

160. (Currently amended) A method as set forth in claim 159, including the step of:

without encrypting the unencrypted electronic message, including, in the transmission between the server and the destination address via the selected one of the SMTP and ESMTP protocols, the identity of the sender, the identity and address of the server and the destination address.

161. (Currently amended) A method as set forth in claim 159, including the steps of:

providing a transmission of the unencrypted electronic message from the server to the sender without encrypting the unencrypted electronic message,

including, in the transmission from the server to the sender, a digital signature of the unencrypted electronic message without encrypting the unencrypted electronic message.

162. (Currently amended) A method as set forth in claim 159, including the step of:

without encrypting the unencrypted electronic message, recording, in the transmission between the server and the destination address via the selected one of the SMTP and ESMTP protocols, the time for the transmission of the unencrypted electronic message from the server to the destination address and the time for the ~~receipt~~ reception of the unencrypted electronic message at the destination address.

163. (Currently amended) A method as set forth in claim 160, including the steps at the server of:

including, in the transmission of the unencrypted message between the server and the sender, a digital signature of the transmission of the unencrypted electronic message between the server and the destination address via the selected one of the SMTP and ESMTP protocols without encrypting the unencrypted electronic message, and recording, in the transmission between the server and the destination address via the selected one of the SMTP and ESMTP protocols, the time for the transmission of the unencrypted message from the server to the destination address and the time for the receipt of the message at the destination address.

164. (Currently amended) A method as set forth in claim 159, including the step at the server of:

including, in the transmission of the unencrypted electronic message between the server and the destination address via the selected one of the SMTP and ESMTP protocols, the status of the delivery of the unencrypted electronic message at the destination address from the server without encrypting the unencrypted electronic message.

165. (Currently amended) A method as set forth in claim 159, including the step of:

receiving at the server a delivery status notification relating to the status of the delivery of the unencrypted electronic message at the destination address and the delivery of the unencrypted electronic message from the destination address to a recipient without encrypting the unencrypted electronic message.

166. (Currently amended) In a method of verifying at a first server a delivery of an unencrypted electronic message to a destination server for a recipient, the steps at the first server of:

transmitting the unencrypted electronic message from the first server to the destination server via a protocol selected from the group consisting of an SMTP protocol and an ESMTP protocol,

receiving, at the first server from the destination server, the transmission between the first server and the destination server of the unencrypted electronic message via the selected one of the SMTP and ESMTP protocols without encrypting the unencrypted electronic message, and

transmitting from the first server to the sender the unencrypted electronic message and the transmission between the first server and the destination server via the selected one of the SMTP and ESMTP protocols without encrypting the unencrypted electronic message protocols.

167. (Currently amended) In a method as set forth in claim 166, the step at the first server of:

without encrypting the unencrypted electronic message, transmitting from the first server to the sender the unencrypted electronic message at the time of the completion of the transmission of the unencrypted electronic message between the first server and the destination server via the selected one of the SMTP and ESMTP protocols.

168. (Currently amended) In a method as set forth in claim 166, the step at the first server of:

without encrypting the unencrypted electronic message, discarding the message at the first server after the transmission of the unencrypted electronic message [[~~in~~]] [[via]] the selected one of the SMPT and ESMPT protocols by the first server to the sender.

169. (Currently amended) In a method as set forth in claim 166, the steps at the first server of:

without encrypting the unencrypted electronic message, providing at the first server a digital signature of the unencrypted electronic message, and

without encrypting the unencrypted electronic message, transmitting the digital signature of the unencrypted electronic message from the first server to the sender at the time of the transmission of the unencrypted electronic message from the first server to the sender.

170. (Currently amended) In a method as set forth in claim 169, the steps at the first server of:

without encrypting the unencrypted electronic message transmitting from the first server to the sender the unencrypted electronic message after the transmission of the unencrypted electronic message between the first server and the destination server via the selected one of the SMTP and ESMTP protocols, and without encrypting the unencrypted electronic message, releasing the unencrypted electronic message at the first server after the transmission of the unencrypted electronic message via the selected one of the SMTP and ESMTP protocols by the first server to the sender.

171 (Currently amended) In a method as set forth in claim 170, the step at the first server of:

without encrypting the unencrypted electronic message, transmitting between the first server and the destination server the identity of the sender, the identity and address of the first server and the identity and address of the destination server and the time of the receipt of the unencrypted electronic message by the first server and the time of the transmission to the first server from the destination server of the identity of the sender, the identity and address of the first server and the identity and address of the destination server.

172 (Currently amended) In a method as set forth in claim 166, the step of:

without encrypting the unencrypted electronic message, receiving at the first server from the destination server a delivery status notification indicating the status of the delivery of the unencrypted electronic message from the first server to the destination server and the time of the transmission of the delivery status notification by the destination server to the first server.

173 (Currently amended) In a method of verifying at a first server a[[n]] unencrypted message received by the first server from a sender and transmitted by the first server to a destination server for a recipient, the steps at the first server of:

without encrypting the unencrypted electronic message receiving at the first server from the destination server an attachment including transmissions between the first server and the destination server relating to the unencrypted electronic message from the sender, the transmissions between the first server and the destination server being provided via a protocol selected from the group consisting of an SMTP protocol and an ESMTP protocol,

without encrypting the unencrypted electronic message, transmitting from the first server to the sender the unencrypted electronic message and the attachment including the transmissions between the first server and the destination server via the selected one of the SMTP protocol and the ESMTP protocol,

without encrypting the unencrypted electronic message, transmitting from the sender to the first server the unencrypted electronic message and the attachment including the transmissions via the selected one of the SMTP and ESMTP protocols, and

authenticating the message on the basis of the unencrypted electronic message and the attachment including the transmission via the selected one of the SMTP and ESMTP protocols.

174. (Currently amended) In a method as set forth in claim 173, wherein:

the attachment includes transmissions between servers intermediate[[~~,~~]] the first server and the destination server.

175. (Currently amended) In a method as set forth in claim 17[[~~0~~]]3, the step at the first server of:

without encrypting the unencrypted electronic message, removing the unencrypted electronic message from the first server when the first server transmits to the sender the unencrypted electronic message and the attachment including the transmissions between the first server and the destination server via the selected one of the SMTP protocol and the ESMTP protocol.

176. (Currently amended) In a method as set forth in claim 173, the steps at the first server of:

without encrypting the unencrypted electronic message receiving at the first server from the destination server the transmission of the identity of the sender, the identity and address of the first server and the identity and address of the destination server via the protocol selected from the group consisting of the SMTP protocol and the ESMTP protocol, and

without encrypting the unencrypted electronic message transmitting from the first server to the sender the identity of the sender, the identity and address of the first server and the identity and address of the destination server at the time of the transmission from the first server to the sender of the unencrypted message and the transmission between the first server and the destination server via the protocol selected from the group consisting of the SMTP protocol and the ESMTP protocol.

177 (Currently amended) In a method as set forth in claim 173, the steps at the first server of

without encrypting the unencrypted electronic message, providing at the first server digital signatures of the unencrypted electronic message and the attachment including the transmission between the first server and the destination server relating to the unencrypted electronic message from the sender, and

without encrypting the unencrypted electronic message, transmitting from the first server to the sender the unencrypted electronic message and the digital signatures of the unencrypted electronic message and the attachment.

178. (Currently amended) In a method as set forth in claim 173, the steps at the first server of:

without encrypting the unencrypted electronic message, transmitting from the first server to the sender the identity of the sender, the identity and address of the first server and the identity and address of the destination server at the time that the unencrypted electronic message and the transmissions between the first server and the destination server are transmitted from the first server to the sender, without encrypting the unencrypted electronic message, transmitting from the sender to the first server the information transmitted from the first server to the sender, and

authenticating the unencrypted electronic message at the first server on the basis of the information transmitted from the sender to the first server and representing the information previously transmitted from the first server to the sender.

179 (Currently amended) A method of verifying delivery at a first server of an encrypted electronic message to a destination server for a recipient, including the steps at the first server of:

receiving at the first server [[~~an~~]] the unencrypted electronic message from a message sender for transmission to the destination server without encrypting the unencrypted electronic message,

without encrypting the unencrypted electronic message, transmitting the unencrypted electronic message from the first server to the destination server via a protocol selected from a group consisting of an SMTP protocol and an ESMTP protocol,

without encrypting the unencrypted electronic message, receiving at the first server the transmissions between the first server and the destination server via the selected one of the SMTP and ESMTP protocols, and

without encrypting the unencrypted electronic message transmitting from the first server to the sender the unencrypted electronic message and at least a particular portion of the transmission[[~~s~~]] between the first server and the destination server via the selected one of the SMTP and ESMTP protocols.

180 (Currently amended) A method as set forth in claim 179 wherein

the unencrypted electronic message and the at least particular portion of the transmissions via the selected one of the SMTP and ESMTP protocols to the sender are provided by the sender to the first server without encrypting the unencrypted electronic message, and wherein

the unencrypted message is authenticated by the first server on the basis of the unencrypted electronic message and the at least particular portion of the transmissions from the sender to the first server.

181. (Currently amended) A method as set forth in claim 17[[~~8~~]][[9]] wherein

a digital signature is provided of the unencrypted electronic message at the first server without encrypting the unencrypted electronic message and wherein

the digital signature is transmitted from the first server to the sender with the message and the at least particular portion of the transmission[[~~s~~]] between the first server and the destination server without encrypting the unencrypted electronic message and wherein

the digital signature is thereafter provided by the sender to the first server with the unencrypted electronic message and the at least particular portion of the transmission[[~~s~~]]

via the selected one of the_SMTP and ESMTP protocols without encrypting the unencrypted electronic message.

182. (Currently amended) A method as set forth in claim 180 wherein

without encrypting the unencrypted electronic message, a digital signature of the unencrypted electronic message and a digital signature of the transmission[[~~s~~]] provided via the selected one of the SMTP and ESMTP protocols are produced at the first server and are transmitted to the sender with the unencrypted electronic message and the transmissions provided [[~~in~~]] via the selected one of the SMTP and ESMTP protocols and wherein

the digital signatures and the unencrypted electronic message and the at least particular portion of the transmission[[~~s~~]] via the selected one of the SMTP and ESMTP protocols to the sender are thereafter provided by the sender to the first server without encrypting the unencrypted electronic message and wherein

without encrypting the unencrypted electronic message, digital fingerprints are produced at the first server from the unencrypted electronic message and the digital signature of the unencrypted electronic message provided by the sender to the first server and wherein

the unencrypted electronic message is authenticated at the first server by establishing an identity between the digital fingerprints produced at the first server.

183. (Currently amended) A method of verifying at a first server the delivery of an unencrypted electronic message from the first server to a destination server ~~for a destination address~~ including the steps of:

without encrypting the unencrypted electronic message, receiving at the first server [[~~an~~]] the unencrypted electronic message from a message sender for transmission to the destination server,

without encrypting the unencrypted electronic message, transmitting the electronic message from the first server to the destination server,

without encrypting the unencrypted electronic message, receiving at the first server the transmission[[~~s~~]] between the first server and the destination server via a protocol selected from the group consisting of the SMTP protocol and the ESMTP protocol,

without encrypting the unencrypted electronic message, transmitting from the first server to the sender the unencrypted electronic message and [[~~the~~]] an unencrypted electronic transmission between the first server and the destination server ~~in~~ via the selected one of the SMTP and ESMTP protocols,

without encrypting the unencrypted electronic message, receiving at the first server from the sender the unencrypted electronic message and the unencrypted electronic transmission between the first server and the destination server [[~~in~~]] via the selected one of the SMTP and ESMTP protocols, and authenticating the unencrypted electronic message at the first server on the basis of the unencrypted electronic message received by the first server from the sender and the unencrypted electronic transmission[[~~s~~]] received by the first server from the sender.

187. (Currently amended) A method as set forth in claim 163, including the steps of:

without encrypting the unencrypted electronic message, transmitting from the sender to the server the unencrypted electronic information transmitted from the server to the sender, and

authenticating the unencrypted electronic message on the basis of the information transmitted from the sender to the server.

188. (Currently amended) A method as set forth in claim 163, including the steps of:

without encrypting the unencrypted electronic message, providing a digital signature of the unencrypted electronic message and a digital signature of an unencrypted electronic attachment including the transmissions between the server and the destination server via the selected one of SMTP and ESMTP the protocols, and

without encrypting the unencrypted electronic message, transmitting the digital signature of the unencrypted electronic message and the digital signature of the attachment from the server to the sender at the same time that the unencrypted electronic message and the unencrypted electronic attachment are transmitted from the server to the sender.

189. (Currently amended) A method as set forth in claim 17[[~~2~~]][[3]], including the steps at the first server of:

generating at the first server a digital signature of the unencrypted electronic message and a digital signature of the unencrypted electronic attachment including the transmission between the first server and the destination server via the selected one of the SMTP and ESMTP protocols without encrypting the unencrypted electronic message, and

transmitting from the first server to the sender the unencrypted electronic message and the unencrypted electronic attachment and the digital signatures of the unencrypted electronic message and the unencrypted electronic attachment without encrypting the unencrypted electronic message.

190. (Currently amended) A method as set forth in claim 173, including the steps at the first server of:

without encrypting the unencrypted electronic message, providing a digital signature of the unencrypted electronic message and a digital signature of the unencrypted electronic attachment including the transmission between the first server and the destination server via the selected one of the SMTP and ESMTP protocols, and without encrypting the unencrypted electronic message, before any authentication of the unencrypted electronic message, transmitting the digital signatures from the first server to the sender at the same time as the transmission from the first server to the sender of the unencrypted electronic message and the unencrypted electronic attachment including the transmission via the selected one of the SMTP and ESMTP protocols.

191. (Currently amended) A method as set forth in claim 189, including the steps at the first server of:

without encrypting the unencrypted electronic message, transmitting from the sender to the first server the unencrypted electronic message and the digital signature of the unencrypted electronic message and the unencrypted electronic attachment and the digital signature of the unencrypted electronic attachment including the transmission[[~~s~~]] between the first server and the destination server via the selected one of the SMTP and ESMTP protocols, and

authenticating the message on the basis of the digital signatures and the unencrypted electronic message and the unencrypted electronic attachment transmitted from the sender to the first server via the selected one of the SMTP and ESMTP protocols.

192. (Previously amended) A method of authenticating a message transmitted from a sender to a recipient, including the steps at the server of:

providing a digital signature of the message,

transmitting the message and the digital signature to the sender,

receiving the message and the digital signature from the sender, and

authenticating the message on the basis of the message and the digital signature received by the server from the sender.

193. (Previously amended) A method as set forth in claim 192, wherein

the server prepares a digital signature of the message and a digital signature of an attachment including an identification of the sender and an identification and address of the server and an identification and address of the recipient and a digital signature of the attachment and wherein

the server transmits to the sender the message and the digital signature of the message and the attachment including the identification of the sender and the identification and address of the server and the identification and address of the recipient and the digital signature of the attachment and wherein

the server receives from the sender the message and the digital signature of the message and the attachment and the digital signature of the attachment and wherein

the server authenticates the message on the basis of the message and the digital signature of the message and the attachment and the digital signature of the attachment all as received by the server from the sender.

194. (Previously amended) A method as set forth in claim 192 wherein

the server prepares a digital signature of the message and an attachment including a selected one of the SMPT and ESMPT protocols involved in the transmission of the message from the server to the recipient and a digital signature of the attachment and wherein

the server transmits to the sender the message and the digital signature of the message and the attachment including the selected one of the SMPT and ESMPT protocols and the digital signature of the attachment and wherein

the server receives from the sender the message and the digital signature of the message and the attachment and the digital signature of the attachment and wherein

the server authenticates the message on the basis of the message and the digital signature of the message received by the server from the sender.

195. (Previously amended) A method as set forth in claim 192 wherein

the server authenticates the message by preparing a digital fingerprint of the message and a digital fingerprint of the digital signature and by comparing the prepared digital fingerprints of the message and the digital signature of the message and confirming that they are identical.

196. (Previously amended) A method as set forth in claim 194 wherein

the server authenticates the message by preparing a digital fingerprint of the message and a digital fingerprint of the attachment including the identification of the sender and the identification and address of the server and the identification and address of the recipient and by comparing the prepared digital fingerprint of the message and the digital signature of the message and confirming that they are identical and by comparing the prepared digital fingerprints of the attachment and the digital signature of the attachment and confirming that they are identical.

197. (Previously amended) A method as set forth in claim 194 wherein

the server authenticates the attachment by preparing a digital fingerprint of the attachment and a digital fingerprint of the digital signature of the attachment including the selected one of the SMPT and ESMPT protocols and by comparing the digital fingerprints and confirming that they are identical.

198. (Previously amended) A method as set forth in claim 194 wherein

the server transmits the message and the attachment and the digital signatures of the message and the attachment to the sender without retaining a copy of the message and the attachment and the digital signatures of the message and the attachment.

199. (Previously amended) A method as set forth in claim 194 wherein

the server transmits to the sender the message and the attachment and the digital signatures of the message and of the attachment and the identification of the sender and the identification and address of the server and the identification and address of the recipient without retaining any of this information.

200. (Previously amended) A method as set forth in claim 197 wherein the server transmits to the sender the message and the digital signature of the message and the attachment including the selected one of the SMPT and ESMPT protocols and the digital signature of the attachment without retaining any of this information.

201. (Previously amended) A method of transmitting a message through the internet from a sender to a recipient through a server displaced from the recipient, including the steps at the server of:

transmitting to the recipient the message and an attachment including an identification of the sender and an identification and address of the server and an identification and address of the recipient,

receiving from the recipient the identification of the sender and an identification and address of the server and an identification and address of the recipient, and

transmitting to the sender the message and the attachment including the identification of the sender and the identification and address of the server and the identification and address of the recipient.

202. (Previously amended) A method as set forth in claim 201 wherein the server prepares a digital signature of the message and transmits the digital signature of the message to the sender with the message.

203. (Previously amended) A method as set forth in claim 202 wherein

the server does not retain a copy of the message and the digital signature of the message when it transmits the message and the digital signature of the message to the sender.

204. (Previously amended) A method as set forth in claim 202 wherein

the server prepares a digital signature of the attachment and transmits this digital signature of the attachment to the sender at the same time that it transmits the attachment to the sender and wherein

the sender transmits to the server the message and the digital signature of the message and the attachment and the digital signature of the attachment when the sender desires to obtain an authentication of the message and the attachment.

205. (Previously amended) A method as set forth in claim 204 wherein

the server provides an authentication of the message and the attachment and the digital signatures of the message and the attachment, all as received by the server from the sender.

206. (Previously amended) A method of transmitting a message through the internet from a sender to a recipient through a server displaced from the recipient, including the steps at the server of:

transmitting to the recipient the message and an identification of the sender and a protocol selected from a group consisting of SMPT and ESMPT protocols.

receiving from the recipient the selected one of the protocols, and

transmitting to the sender the message and the selected one of the protocols.

207. (Previously presented) A method as set forth in claim 206, including the steps of:

preparing at the server a digital signature of the message, and

transmitting the digital signature from the server to the sender with the message.

208. (Previously amended) A method as set forth in claim 206, including the step of:

not retaining at the server a copy of the message and the digital signature of the message when the server transmits the message and the digital signature of the message to the sender.

209. (Previously amended) A method as set forth in claim 206, including the step of:

preparing at the server a digital signature of the message and a digital signature of the selected one of the protocols, and

transmitting the digital signatures from the server to the sender with the message and the selected one of the protocols.

210. (Previously amended) A method as set forth in claim 207, including the steps of:

preparing at the server a digital signature of the [message and] of the selected one of the protocols, and

transmitting the digital signature of the message from the server to the sender with the message and the digital signature of the selected one of the protocols with the protocol, and

not retaining at the server a copy of the message and the digital signature of the message and the selected one of the protocols and the digital signature of the selected one of the protocols when the server transmits the message and the digital signature of the message and the selected one of the protocols and the digital signature of the selected one of the protocols to the sender.

211. (Previously presented) A method as set forth in claim 208, including the steps of:

transmitting the message and the digital signature of the message from the sender to the server, and

authenticating the message on the basis of the message and the digital signature transmitted from the sender to the server.

212. (Previously presented) A method as set forth in claim 210, including the steps of:

transmitting from the sender to the server the message, the digital signature of the message, the attachment and the digital signature of the attachment, and

authenticating the message on the basis of the message and the digital signature of the message transmitted from the sender to the server and authenticating the attachment on the basis of the attachment and the digital signature of the attachment transmitted from the sender to the server.

213. (Previously presented) In a method of authenticating a message transmitted through the internet by a server from a sender to an agent of a recipient, the steps at the server of:

transmitting to the recipient the message and an attachment including the identity of the sender and the identity and address of the server and the identity and address of the recipient, and

receiving the indication by the agent of the receipt of the message by the agent, and

including the indication of the receipt of the message by the agent in the attachment.

213. (Previously presented) In a method as set forth in claim 213, the step at the server of:

creating a digital signature of the message and a digital signature of the attachment.

215. (Previously presented) In a method as set forth in claim 214, the step at the server of:

transmitting to the sender the message and the digital signature of the message and the attachment and the digital signature of the attachment.

216. (Previously presented) In a method as set forth in claim 215, the step at the server of:

receiving from the sender the message and the attachment and the digital signatures of the message and the attachment.

217. (Previously presented) In a method as set forth in claim 216, the step at the server of:

authenticating the message on the basis of the message and the attachment and the digital signature of the message and the attachment, all as received by the server from the sender.

218. (Previously presented) In a method of authenticating a message transmitted through the internet by a server from a sender to an agent of recipient, the steps at the server of:

receiving from the agent a protocol selected from a group consisting of SMPT and ESMPT protocols after the transmission of the message from the server to the agent of the message by the selected one of the protocols, and

providing at the server a digital signature of the message, and

transmitting the message and the digital signature of the message from the server to the sender.

219. (Previously presented) In a method as set forth in claim 218, the step of:

disposing of the message and the digital signature of the message at the server after the transmission of the message and the digital signature of the message from the server to the sender.

220. (Previously presented) In a method as set forth in claim 219, the steps of:

receiving at the server the message and the digital signature of the message after the disposition of the message and the digital signature of the message at the server, and

authenticating the message at the server on the basis of the message and the digital signature of the message received by the server from the sender.

221. (Previously presented) In a method as set forth in claim 218, the steps of:

providing an attachment including the selected one of the protocols,

providing a digital signature of the attachment, and

transmitting from the server to the sender the attachment and the digital signature of the attachment at the same time as the transmission of the message and the digital signature of the message from the server to the sender.

222. (Previously presented) In a method as set forth in claim 221, the step of:

disposing of the message and the attachment and the digital signature of the message and the attachment at the server after the transmission of the message and the digital signature of the message and the attachment and the digital signature of the attachment from the server to the sender.

223. (Previously presented) In a method as set forth in claim 222, the steps of:

receiving at the server from the sender the message, the attachment and the digital signatures of the message and the attachment after the disposition of the message and the digital signature of the message and the attachment and the digital signature of the attachment at the server, and

authenticating the message and the attachment at the server on the basis of the message and the digital signature of the message and the attachment and the digital signature of the attachment, all as received at the server from the sender.

224. (Previously presented) In a method as set forth in claim 220 wherein the authentication is provided by generating at the server a digital fingerprint of the message, and a digital fingerprint of the digital signature of the message, received by the server from the sender and comparing the digital fingerprints generated at the server.

225. (Previously presented) In a method as set forth in claim 223 wherein the authentication is provided as follows:

generating at the server a digital fingerprint of the message from the message received by the server from the sender, and a digital fingerprint of the digital signature of the message received at the server, and comparing the digital fingerprints generated at the server, and

226. (Currently amended) In a method of authenticating a[[n]] unencrypted message provided by a sender and transmitted to a destination server by a second server displaced from the sender and the destination server, the steps at the second server of:

without encrypting the unencrypted electronic message, providing an unencrypted electronic attachment transmitted between the second server and the destination server via a selected one of SMTP and ESMTP protocols, and

transmitting the unencrypted electronic attachment from the second server to the sender without encrypting the unencrypted electronic message or the unencrypted electronic attachment.

227. (Currently amended) In a method as set forth in claim 226, the steps at the second server of:

providing a digital signature of the unencrypted electronic attachment at the second server without encrypting the unencrypted electronic message or the unencrypted electronic attachment, and

without encrypting the unencrypted electronic message or the unencrypted electronic attachment, transmitting the digital signature[[s]] or the unencrypted electronic message and from the second server to the sender at the time of transmitting the unencrypted electronic attachment from the second server to the sender.

228. (Currently amended) In a method as set forth in claim 227, the steps at the second server of:

without encrypting the unencrypted electronic attachment, receiving the unencrypted electronic attachment and the digital signature of the unencrypted electronic attachment at the second server from the sender, and

authenticating the attachment at the second server on the basis of the unencrypted electronic attachment and the digital signature received by the second server from the sender of the unencrypted electronic attachment.

229. (Currently amended) In a method as set forth in claim 227, the steps at the second server of:

receiving the unencrypted electronic attachment and the digital signature of the unencrypted electronic attachment at the second server from the sender without encrypting the unencrypted electronic message, without encrypting the unencrypted electronic attachment, providing at the second server digital fingerprints of the unencrypted electronic attachment and the digital signature received at the second server from the sender of the unencrypted electronic attachment, and

comparing the digital fingerprints to authenticate the unencrypted electronic attachment.

230. (Currently amended) In a method of authenticating a[[n]] unencrypted message provided by a sender and transmitted to a destination server by a second server displaced from the sender and the destination server, the steps at the second server of:

without encrypting the unencrypted electronic message, providing an unencrypted electronic attachment including the identity and address of the sender and the identity and address of the second server and the identity and address of the destination server, and

transmitting the unencrypted electronic attachment from the second server to the sender without encrypting the unencrypted electronic attachment.

231. (Currently amended) In a method as set forth in claim 230 wherein

the unencrypted electronic attachment includes the address and identity of intermediate stations receiving the unencrypted electronic attachment in the transmission of the unencrypted electronic ~~message~~ attachment between the second server and the destination server.

232. (Currently amended) In a method as set forth in claim 230, the steps at the second server of:

providing a digital signature of the unencrypted attachment at the second server without encrypting the unencrypted attachment, and

without encrypting the unencrypted attachment, transmitting the digital signature of the unencrypted attachment from the second server to the sender[[,]] at the time of transmitting the unencrypted attachment from the second server to the sender.

233. (Currently amended) In a method as set forth in claim 231, the steps at the second server of:

providing a digital signature of the unencrypted attachment at the second server without encrypting the unencrypted attachment, and

without encrypting the unencrypted attachment, transmitting the digital signature of the unencrypted attachment from the second server to the sender[[,]]at the time of transmitting the unencrypted attachment from the second server to the sender.

234. (Currently amended) In a method as set forth in claim 232, the steps at the second server of:

without encrypting the unencrypted attachment, receiving the unencrypted attachment and the digital signature unencrypted attachment at the second server from the sender, and authenticating the unencrypted attachment at the second server on the basis of the unencrypted attachment and the digital signature received by the second server from the sender of the unencrypted attachment.

235. (Currently amended) In a method as set forth in claim 233, the step[[~~s~~]] at the second server of:

authenticating the unencrypted attachment at the second server on the basis of the unencrypted attachment and the digital signature received by the second server from the sender of the encrypted attachment.

236. (Currently amended) In a method as set forth in claim 232, the steps at the second server of:

receiving the unencrypted attachment and the digital signature at the second server of the unencrypted attachment from the sender without encrypting the unencrypted attachment,

without encrypting the unencrypted electronic message, providing at the second server digital fingerprints of the unencrypted attachment and the digital signature received at the second server from the sender of the unencrypted attachment, and

comparing the digital fingerprints at the second server to authenticate the attachment.

237. (Currently amended) In a method as set forth in claim 233, the steps at the second server of:

receiving the unencrypted attachment and the digital signature of the encrypted attachment at the second server from the sender,

without encrypting the unencrypted attachment, providing at the second server digital fingerprints of the unencrypted attachment and the digital signature received at the second server from the sender of the unencrypted attachment , and

comparing the digital fingerprints to authenticate the attachment.

238 (Currently amended) In a method of ~~verifying~~ authenticating at a server [[~~a~~]] an unencrypted electronic message and delivery of [[~~an~~]] the unencrypted electronic message to a destination address, the steps of:

transmitting the unencrypted electronic message between the server and the destination address without encrypting the unencrypted electronic message.,

receiving at the server the path of transmission of the unencrypted message between the server and the destination address without encrypting the unencrypted electronic message, the path including servers between the server and the destination address, and

without encrypting the unencrypted electronic message, transmitting to the sender the unencrypted electronic message and the path of transmission of the unencrypted electronic message between the server and the destination [[~~or~~]] address.

239. (Currently amended) In a method as set forth in claim 238 wherein

the server does not retain the unencrypted message or the path of transmission of the unencrypted message between the server and the destination address after the server transmits to the sender the unencrypted message and the path of transmission of the message between the server and the destination address.

240. (Currently amended) In a method as set forth in claim 238 wherein

without encrypting the unencrypted electronic message, the server receives from the sender the unencrypted message and the path of transmission of the unencrypted message between the server and the destination address and wherein

the server authenticates the unencrypted message on the basis of the receipt by the server from the sender of the unencrypted message[[~~,~~]] and the path of transmission of the unencrypted message between the server and the destination address~~, received by the server from the sender~~.

241. (Currently amended) In a method as set forth in claim 240 wherein

the server provides a digital signature of the unencrypted message and transmits the digital signature with the unencrypted message to the sender and wherein

the server receives from the sender the unencrypted message and the digital signature of the unencrypted message and wherein

the server provides digital fingerprints of the unencrypted message and the digital signature and compares the digital fingerprints to authenticate the unencrypted message.

242. (Currently amended) In a method as set forth in claim 240 wherein

the server provides a digital signature of the path of transmission of the unencrypted message between the server and the destination address and transmits the digital signature to the sender with the path of transmission and wherein

the server receives from the sender the path of transmission and the digital signature of the path of transmission and wherein

the server provides digital fingerprints of the path of transmission and the digital signature of the path of the transmission and compares the digital fingerprints to authenticate the unencrypted message.

PLEASE ADD THE FOLLOWING NEW CLAIMS

243. (New) A method of providing a delivery at a server of an unencrypted message from the server to a designated address, including the steps at the server of:

receiving at the server the unencrypted message from a sender for transmission to the designated address without encrypting the unencrypted message,

transmitting the unencrypted message from the server to the designated address via a particular protocol without encrypting the unencrypted message, and

without encrypting the unencrypted message, receiving at the server the transmission of the unencrypted message between the server and the designated address via the particular protocol before any authentication of the unencrypted message.

244. (New) A method set forth in claim 243, including the steps at the server of

without encrypting the unencrypted message, providing a digital signature of the unencrypted message, and

without encrypting the unencrypted message, providing for the transmission from the server to the sender of the unencrypted message and the digital signature of the unencrypted message,

245. (New) A method as set forth in claim 244, including the step as the server of:

without encrypting the unencrypted message, providing a reception at the server of the unencrypted message, and the digital signature of the unencrypted message, from the sender.

246. (New) A method as set forth in claim 244, indicating the step of the server of:

authenticating the unencrypted message at the server on the basis of the unencrypted message, and the digital signature of the unencrypted message, received at the server from the sender.

247. (New) A method as set forth in claim 245, including the steps at the server of:

without encrypting the unencrypted message, providing digital fingerprints of the digital signature and of the unencrypted message, and

comparing the digital fingerprints to authenticate the unencrypted message.

248. (New) A method as set forth in claim 243, including the step at the server of:

without encrypting the unencrypted message, receiving at the server an unencrypted attachment identifying intermediate stations between the server and the designated address, the intermediate stations being operative to provide for the transmission of the unencrypted message between the server and the designated address,

249. (New) A method as set forth in claim 248, including the step at the series of:

providing for the transmission from the server to the sender of the unencrypted message and the unencrypted attachment without encrypting the unencrypted message, and

providing for the destruction or discarding at the server of the unencrypted message and the unencrypted attachment without encrypting the unencrypted message and the unencrypted attachment,

providing for the transmission from the sender to the server of the unencrypted message and the unencrypted attachment, and

providing for the authentication at the server of the unencrypted message and the unencrypted attachment on the basis of the unencrypted message, and the unencrypted attachment, received by the server from the sender.

250. (New) A method as set forth in claim 248, including the steps at the server of:

without encrypting the unencrypted message and the unencrypted attachment providing for the transmission from the server to the sender of the unencrypted message and the unencrypted attachment and a selection of (a) a digital signature of the unencrypted message and a digital signature of the unencrypted attachment and (b) a digital signature of a combination of the unencrypted message and the unencrypted attachment, and

without encrypting the unencrypted message but at the same time as the transmission of the unencrypted message and the unencrypted attachment and the selected one of (a) the digital signature of the unencrypted message and the digital signature of the unencrypted attachment and (b) the digital signature of the combination of the unencrypted message and the unencrypted attachment, discarding the unencrypted message and the attachment and the selected one of (a) the digital signature of the unencrypted attachment and (b) the digital signature of the combination of the unencrypted message and the unencrypted attachment.

251. (New) In a method as set forth in claim 249, the steps at the server of:

without encrypting the unencrypted message, receiving from the sender the unencrypted message and the unencrypted attachment and the selected one of (a) the digital signature of the unencrypted message and the digital signature of the unencrypted attachment and (b) the digital signature of the combination of the unencrypted message and the unencrypted attachment, and

authenticating the unencrypted message and the unencrypted attachment on the basis of the unencrypted message and the unencrypted attachment and the selected one of (a) the digital signature of the unencrypted message and the digital signature of the unencrypted attachment and (b) the digital signature of the combination of the unencrypted message and the unencrypted attachment.

252. (New) A method as set forth in claim 251 wherein

digital fingerprints are provided at the server of the unencrypted message and of the unencrypted attachment and of the selected one of (a) the digital signature of the unencrypted message and the digital signature of the unencrypted attachment and (b) the digital signature of the combination of the unencrypted message and the unencrypted attachment.

253. (New) A method as set forth in claim 251 wherein

digital fingerprints are provided at the server of (a) the unencrypted message and (b) the unencrypted attachment, (c) the digital signature of the unencrypted message and, (d) the digital signature of the unencrypted attachment when digital signatures are provided at the server of the unencrypted message and the attachment and wherein

to authenticate the unencrypted message, the digital fingerprints of the unencrypted message and the digital signature of the unencrypted message are compared and

the digital fingerprints of the unencrypted attachment and the digital signature of the unencrypted attachment are compared to authenticate the unencrypted attachment.

254. A method as set forth in claim 251 wherein,

digital fingerprints are provided at the server of the combination of the unencrypted message and the unencrypted attachment and the digital signature of the combination of the unencrypted message and the unencrypted attachment and wherein

the digital fingerprint of the combination of the unencrypted message and the unencrypted attachment is compared with the digital fingerprint of the digital signature of the combination of the unencrypted message and the unencrypted attachment to authenticate the unencrypted message.

255. (New) In a method as set forth in claim 115, the steps at the server of:

without encrypting the unencrypted message, receiving an unencrypted attachment from the destination address, providing at the server a digital signature of a combination of the unencrypted message and the unencrypted attachment, and

without encrypting the unencrypted message and the unencrypted attachment, transmitting to the sender the unencrypted message, the unencrypted attachment and the digital signature of the combination of the unencrypted message and the unencrypted attachment.

256. (New) In a method as set forth in claim 255, the steps at the server of:

without encrypting the unencrypted message, generating a digital fingerprint of a combination of the unencrypted message and the unencrypted attachment and a digital fingerprint of the digital signature of the combination of the unencrypted message and the unencrypted attachment, and

comparing the digital fingerprints to authenticate the message and the attachment.

257. (New) In a method as set forth in claim 256 wherein

the unencrypted attachment includes intermediate stations providing a

transmission of the unencrypted message between the server and the destination address.

258. (New) In a method as set forth in claim 255, the steps at the server of:

without encrypting the unencrypted message, receiving from the sender copies of the unencrypted message, the unencrypted attachment and the digital signature of the combination of the unencrypted message and the unencrypted attachment, and authenticating the unencrypted message and the unencrypted attachment on the basis of the unencrypted message, the unencrypted attachment and the digital signature of the combination of the unencrypted message and the attachment, and

the attachment identifying the intermediate stations providing for the transmission of the unencrypted message between the server and the destination address.

259. (New) In a method as set forth in claim 257, the step at the server of:

receiving at the server a delivery status notification relating to the status of the unencrypted message at the destination address and the status of the delivery of the unencrypted message from the destination address to a recipient at the destination address.

260. (New) A method as set forth in claim 263, including the step of:

without encrypting the unencrypted message, receiving at the server from the designated address a delivery status notification indicating the status of the delivery of the unencrypted message from the server to the designated address and the time of the transmission of the status notification from the designated address to the server.

261. (New) In a method as set forth in claim 173, the steps of:

without encrypting the unencrypted message, transmitting from the first server to the sender the unencrypted message, the unencrypted attachment and the digital signature of the combination of the unencrypted message and the unencrypted attachment, and without encrypting the unencrypted message, transmitting from the first server to the sender the unencrypted message, the unencrypted attachment and the digital signature of the combination of the unencrypted message and the unencrypted attachment.

262. (New) A method as set forth in claim 243 wherein:

the destination address is one of a plurality of destination addresses receiving the unencrypted message from the server and wherein

the server identifies each individual one of the destination addresses in transmitting the unencrypted message to the destination address.

263. (New) A method as set forth in claim 250 wherein:

the destination address is one of a plurality of destination addresses receiving the unencrypted message from the server and wherein

the server identifies each individual one of the destination addresses in transmitting the unencrypted message to the destination address.

264. (New) A method as set forth in claim 247 wherein:

the attachment includes the identity and address of the sender, the identity and address of the server and the designated address.

265. (New) A method as set forth in claim 248 wherein:

the attachment includes the identity and address of the sender, the identify and address of the server and the designated address.

266. A method as set forth in claim 250 wherein

the unencrypted message and the unencrypted attachment are transmitted from the server to the sender via a selected one of an SMTP protocol and an ESMTP protocol and wherein

the server receives from the sender the unencrypted message and the unencrypted attachment via the selection of one of the SMTP and ESMTP protocols.

267. (New) A method as set forth in claim 255 wherein:

via a selected one of the SMTP and ESMTP protocols, the unencrypted message and the unencrypted attachment are received at the server from the destination address, are transmitted by the server to the sender and are received by the server from the sender.

268. (New) A method as set forth in claim 249 wherein:

the time for the transmission of the unencrypted message from the server to the designated address and the time for the reception of the unencrypted message at the designated address are provided at the server and wherein

without encrypting the unencrypted message, the time of the transmission of the unencrypted message from the server to the destination address and the time for the reception of the unencrypted message at the destination address are included in the transmission from the server to the sender.

269. (New) A method as set forth in claim 261 wherein

without encrypting the unencrypted message, the time for the transmission of the unencrypted message from the server to the designated address and the time for the reception of the unencrypted message at the designated address are transmitted from the server to the sender.

270. A method of providing proof of the delivery of a message comprising the steps of:

receiving from a sender across a computer network an unencrypted electronic message, the unencrypted electronic message having a destination address associated therewith;

transmitting, via a selected one of SMTP and ESMTP protocols, the unencrypted electronic message from a transmitting server to a receiving server associated with the destination address;

recording, at least a portion of data exchanged between the transmitting server and the receiving server in the course of transmission via the selected one of the SMTP and ESMTP protocols, said record defining a dialog between the transmitting and receiving servers via the selected one of the SMTP and ESMTP protocols; and

transmitting the record to a storage means displaced from the transmitting and receiving server, to provide a proof at a later date of the delivery of the unencrypted electronic message to the receiving server by the transmitting server.

271. The method of claim 270 further comprising the steps of:

transmitting the unencrypted electronic message via the selected one of the SMTP and ESMTP protocols to a plurality of additional receiving servers associated with additional destination addresses;

recording dialogs corresponding to the transmission of the message to the additional destination servers via the selected one of the SMTP and ESMTP protocols; and

transmitting the records to storage means displaced from the transmitting server and the receiving server to provide for the production of the dialogs at a later date as proof of the delivery of the unencrypted electronic message to the receiving servers by the transmitting server.

272. The method of claim 270 wherein

the method of storage comprises transmitting a copy of the recorded dialog to the sender of the unencrypted electronic message, the copy defining a Delivery Receipt of the unencrypted electronic message.

273. The method of claim 272 including the step of:

digitally signing the delivery receipt with an encryption key which is not known to the sender of the unencrypted electronic message.

274. The method of claim 270 wherein

the unencrypted electronic message is transmitted through the internet between the transmitting server and the receiving server and wherein the addresses of the transmitting server and the receiving server are e-mail addresses.

275. A method of providing proof of the delivery of a message comprising the steps of:

receiving from a sender across a computer network an unencrypted electronic message, the electronic message having a destination address associated therewith;

creating a fictitious address composed of a unique identifier of the unencrypted electronic message, a unique identifier of the destination address of the unencrypted electronic message and a domain name of a server designated as the Receipt Server;

transmitting the unencrypted electronic message, via a selected one of an SMTP protocol and an ESMTP protocol, by a transmitting server to a receiving server associated with the destination address;

in the course of said transmission, directing the receiving server to send to the fictitious address a Delivery Status Notification (DSN) for the unencrypted electronic message in compliance with the selected one of the SMTP protocol and the ESMTP protocol;

receiving, at the Receipt Server a Delivery Status Notification containing a notice of the delivery status of the unencrypted electronic message addressed to the fictitious address; and transmitting at a later date at least one of the Delivery Status Notification and a digest thereof to a storage means displaced from the transmitting server and the receiving server to provide proof of the delivery of the unencrypted electronic message to the receiving server by the transmitting server.

276. The method of claim 275 further comprising the steps of:

transmitting the unencrypted electronic message to a plurality of additional receiving servers associated with additional destination addresses;

receiving at the Receipt Server Delivery Status Notifications containing a notice of the delivery status of the unencrypted electronic message to each of the additional destination addresses, and

transmitting at least one of the Delivery Status Notification and a digest thereof to a storage means displaced from the transmitting server and the receiving servers to provide proof at a later date of the delivery of the unencrypted electronic message to the receiving servers by the transmitting server.

277. The method of claim 276 wherein

the method of storage comprises sending a copy of at least one of the DSN Message and

a digest thereof to the original sender of the message, said copy defining a Delivery Receipt for the unencrypted electronic message.

278. The method of claim 273 including the step of digitally signing the delivery receipt

with an encryption key which is not known to the sender of the unencrypted electronic message.

279. The method of claim 276 wherein

the unencrypted electronic message is transmitted through the internet to the receiving server and the additional receiving servers and wherein

the receiving server and the additional receiving servers are constructed to receive e-mail.

280. A method of providing proof regarding the delivery of an unencrypted electronic

message to a recipient comprising the steps of:

receiving from a sender across a computer network an unencrypted electronic message having a destination address associated therewith;

creating a fictitious address composed of a unique identifier of the unencrypted electronic message, a unique identifier of the destination address of the unencrypted electronic message and a domain name of a server, the fictitious address being designated as the Receipt Server;

adding to the unencrypted electronic message a message header which directs a mail client of the recipient to send a notification message to the fictitious address upon the opening of the unencrypted electronic message; and receiving, at the Receipt Server, a notification message of the opening of the unencrypted electronic message addressed to the fictitious address; and

transmitting at least one of the notification message and a digest thereof to a storage means to provide proof at a later date of the delivery of the unencrypted electronic message to the recipient, the storage means being displaced from the Receipt Server and the destination address.

281. The method of claim 280 further comprising the steps of:

transmitting copies of the unencrypted electronic message to a plurality of destination servers having to delivery addresses associated with the unencrypted electronic message, each copy of the unencrypted electronic message bearing a fictitious address distinctive of its respective destination address; and

receiving at the Receipt Server a notification of the opening of the message at each of the delivery addresses, each such notification being addressed to the fictitious address at the Receipt Server.

282. A method as set forth in 280, including the step of:

transmitting at least one of the notification messages and a digest thereof to a storage means displaced from the Receipt Server and the destination server to provide proof at a later date of the delivery of the unencrypted electronic message to the recipient.

283. The method of claim 281 wherein

the method of storage comprises sending a copy of at least one of the notification message and a digest thereof to the sender of the unencrypted electronic message, the copy defining a Delivery receipt for the unencrypted electronic message.

284. The method of claim 283 including the step of:

digitally signing the delivery receipt with an encryption key which is not known to the sender of the message.

285. The method of claim 283 wherein

the unencrypted electronic message is transmitted through the internet to the recipient's mail client, the recipient's mail client being responsive to the unencrypted electronic message transmitted through the internet and being an e-mail server.